UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/478,796	01/07/2000	NAREN CHAGANTI	PSCO-005	2169

7590 02/13/2004

LAW OFFICES OF NAREN CHAGANTI
345 SHERIDAN AVENUE
APT 308
PALO ALTO, CA 94306

EXAMINER	
DARROW, JUSTIN T	

ART UNIT	PAPER NUMBER
2132	39

DATE MAILED: 02/13/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/478,796	CHAGANTI ET AL.	
	Examiner	Art Unit	
	Justin T. Darrow	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on *12 December 2003*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *48-77* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *48,49,52-75 and 77* is/are rejected.

7)☒ Claim(s) *50, 51, and 76* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *07 January 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-77 have been presented for examination. Claims 1-6 have been originally filed 01/07/2000. Claim 1 has been amended, claim 6 has been canceled, and new claims 7-30 have been added in an amendment filed 05/19/2000. Claims 1, 5, 14, 19, 22, 23, and 25-30 have been amended and new claims 31-43 have been added in an amendment filed 11/13/2000. Claims 31-43 have been canceled in an amendment filed 02/21/2001. Claims 1-4, 7-11, 18, 23, and 26-30 have been amended; claims 12, 13, and 25 have been canceled; and new claims 44-47 have been added in an amendment filed 11/06/2002. Claims 1, 5, 15, and 20-22 have amended in an amendment filed 02/24/2003. Claims 1-5, 7-11, 14-24, 26-30, and 44-47 have been canceled and new claims 48-77 have been added in an amendment filed 04/08/2003. Claims 69, 72, and 73 have been amended in an amendment filed 12/12/2003. Claims 48-77 have been examined.

Request to Refund Petition Fee for Extension of Time

2. Examiners have no authority to grant a request for a refund for a petition fee paid for an extension of time. The applicant must file a petition under 37 CFR 1.181 to be decided by the technology center director. See MPEP § 1002.02(c) 3. (i) petition for resetting period for reply, MPEP § 710.06.

Request for Interview Before Next Office Action

3. An interview must be arranged for in advance of the filing of the response to the last Office action. See MPEP § 713.01. Further, the applicant must file an "Applicant Initiated Interview Request" form (PTOL-413A). See

http://www.uspto.gov/web/forms/index.html#startforms . Because no interview has been arranged in advance, no interview is possible before this Office action.

Response to Arguments

4. Applicant's arguments filed 12/12/2003 have been fully considered but they are not persuasive.

5. As per claim 48, Fortenberry et al., U.S. Patent No. 6,005,939 A does disclose the limitation:

assigning, by the first party, at least one of a plurality of security levels to each information object at any granularity(see column 7, lines 24-30; figure 3, items 304 and 306; security level is assigned to each item of the user information included in the passport data field; see column 7, lines 45-51; figure 4, items 406, 408, and 410; the user responds to a series of queries by entering requested information and choosing security levels to be assigned to each item of requested information; see column 7, lines 53-60; security levels assigned to each item of user information range from highly secure to public, for a high security level of 100 on an exemplary scale of 0-100 levels to public level 0),

enabling access to individually selected portions of the first party's personal information by individual receiving parties (see column 8, lines 1-7; security keys are delivered to the passport requestor to access information that may be granted at various levels such as real-ID (very secure), virtual-ID and less private information classes; see column 8, lines 40-64; figure 2, items 216; figure 5, process blocks 512, 514, 518, and 520; based on the security level of the identified information, the passport agent determines whether or not the requested information

should be transmitted to the vendor in encrypted form, where the vendor may decrypt the encrypted identified information of the passport only if it is sent the particular public key by the user corresponding to the security level of that identified information).

In this claim, "by the first party" clearly refers to the user in Fortenberry et al. Fortenberry et al. additionally embody "assignment of security levels at any granularity" by describing security levels assigned to each item ranging from highly secure to public, for a high security level of 100 on an exemplary scale of 0-100 levels to public level 0. Also, Fortenberry et al. discuss "security levels can be assigned so as to allow individually selected portions of the information objects to be released to different receiving parties" by mentioning a message as follows: RELEASY SOCIAL-SECURITY-NUMBER TO WEB-SITE-X ON BEHALF OF MY-USER-ID, where the vendor corresponding to web-site-X can only decrypt the social security number if it has obtained the public key corresponding to the private key, of the security level assigned to the social security number, used to encrypt the social security number.

6. As per claim 63, Fortenberry et al. anticipates claim 63 by describing only one of the alternative embodiments explicitly recited in claim 63. Because claim 63 is of the form "includes A; B; C; . . . ; I; or J," claim 63 is a Markush-type claim representing alternative embodiments. See MPEP § 2173.05(h) I. A Markush-type claim is anticipated if a prior art reference discloses at least one of the alternative embodiments. See MPEP § 2131.02. See *In re Gosteli*, 10 USPQ2d 1614 (Fed. Cir. 1989) (ruling that a prior art reference disclosing two of 21 species in Markush claims anticipated the claims under 35 U.S.C. § 102(e) unless the claims were entitled to the priority date of a foreign application under 35 U.S.C. § 112, ¶ 1). Because of the administrative burden of citing cumulative references to render obvious each alternative

embodiment in claim 63, claim 63 was rejected based on the legally sufficient description of four of the fourteen alternatives in Fortenberry et al.

7. As per claim 74, Fortenberry et al. does disclose:

generating an authorization key (see column 7, lines 24-33; figure 3, item 308; figure 4, process 416; storing generated keys for encryption and decryption in a key field and assigning an encryption key);

providing the authorization key to the second party (see column 8, lines 1-7; security keys for each item at different security levels are delivered to the passport requestor); and

encoding the authorization key with at least one of a plurality of criteria (see column 8, lines 1-7; security keys for each item at different security levels are delivered to the passport requestor; see column 9, lines 8-10; the public and private keys described herein may be encrypted using the double keying encryption technology currently known in the art).

Fortenberry et al. embodies "generating" the authorization key, which corresponds to the public key the vendor must use to decrypt the encrypted identified information of the passport where the public key corresponds to the security level of that identified information. Fortenberry et al. further specify "encoding" the authorization key by elaborating on double keying encryption. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., "user-defined authorization key generated at the time and for the purpose of the transaction") are not recited in the rejected claims. Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

As per claims 52, 61, 62, 66, 67, and 71-73, Fortenberry et al. in view of the various secondary references renders obvious these claims and includes motivation explicitly provided by the respective secondary reference, as explained in the grounds of rejection below in this Office action.

Drawings

8. The drawings filed on 01/07/2000 are acceptable as indicated on the "Notice of Draftperson's Patent Drawing Review," PTO-948, attached to Paper No. 26.

Claim Rejections - 35 USC § 102

9. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

10. Claims 48, 49, 53-60, 63-65, 68-70, 74, 75, and 77 are rejected under 35 U.S.C. 102(e) as being anticipated by Fortenberry, U.S. Patent No. 6,005,939 A.

As per claim 48, Fortenberry et al. illustrate a method for disbursing a first party's personal information comprising:

establishing an account for the first party with a server computer coupled to a database (see column 5, lines 65-67; column 6, lines 1-5; figure 2A, items 208, 212, 214, and 216; users can store personal and optional demographic information in passport database where it is entered once; see column 7, lines 39-41; figure 4, process 400; user sends a request to generate a passport to passport agent);

assigning an identifier to the first party (see column 6, lines 26-29; user has previously provided to web site a public key to identify and decode data provided by passport agent; see column 7, lines 60-62; figure 4, process 418; passport agent provides a public key to the user to access the passport data);

entering the first party's personal information comprising at least one of a plurality of information objects (see column 6, lines 52-55; figure 3, item 305; real information about a user such as the user's real name, address, credit card information, social security number, etc.; column 6, lines 63-67; column 7, lines 1-9; figure 3, item 305; virtual information includes user's preferences);

assigning, by the first party, at least one of a plurality of security levels to each information object at any granularity(see column 7, lines 24-30; figure 3, items 304 and 306; security level is assigned to each item of the user information included in the passport data field;

see column 7, lines 45-51; figure 4, items 406, 408, and 410; the user responds to a series of queries by entering requested information and choosing security levels to be assigned to each item of requested information; see column 7, lines 53-60; security levels assigned to each item of user information range from highly secure to public, for a high security level of 100 on an exemplary scale of 0-100 levels to public level 0),

enabling access to individually selected portions of the first party's personal information by individual receiving parties (see column 8, lines 1-7; security keys are delivered to the passport requestor to access information that may be granted at various levels such as real-ID (very secure), virtual-ID and less private information classes; see column 8, lines 40-64; figure 2, items 216; figure 5, process blocks 512, 514, 518, and 520; based on the security level of the identified information, the passport agent determines whether or not the requested information should be transmitted to the vendor in encrypted form, where the vendor may decrypt the encrypted identified information of the passport only if it is sent the particular public key by the user corresponding to the security level of that identified information);

storing in the database the first party identifier, the information object and the security level assigned to the information object (see column 6, lines 47-51; figure 3, items 304, 305, 306, 308; passport portion in the passport agent includes fields; see column 6, lines 52-65; figure 3, item 305; first field for user identifying and virtual information; see column 7, lines 24-25; figure 3, item 306; second field corresponding to a security level field; see column 7, lines 31-33; figure 3, item 308; a key field for one or more keys for identifying the data along with the user name);

receiving a request comprising at least the first party identifier (see column 8, lines 37-52; figure 5, process block 508; request for information on behalf of MY-USER-ID);

in response to the request, selecting a first portion of the first party's personal information objects that could be transmitted to a second party (see column 8, lines 46-51; figure 2, item 216; figure 5, process block 512; passport agent determines whether or not the requested information should be transmitted to the vendor in encrypted form); and

securely transmitting the retrieved first portion of personal information objects to the second party (see column 8, lines 54-64; figure 5, process blocks 514 and 516; passport agent encrypts information and vendor receives encrypted information).

As per claim 49, Fortenberry et al. further elaborate on:

presenting an authorization by the second party (see column 8, lines 37-42; vendor requests: RELEASE-TYPE TO INTERNET-SITE ON BEHALF OF MY-USER-ID); and

verifying the second party's authorization (see column 8, lines 46-51; figure 5, process block 512; passport agent determines whether or not the requested information should be transmitted to the vendor in encrypted form).

As per claim 53, Fortenberry et al. additionally describe:

generating an authorization key (see column 8, lines 17-20; encryption method with public and private keys so that the public key is given to the user to access passport data; see column; see column 8, lines 40-42; MY-USER-ID); and

providing the authorization key to the second party (see column 8, lines 31-32; figure 5, process block 504; user provides a public key to the vendor; see column 8, lines 59-64; figure 5,

process block 518; the public key sent by the user is used to unlock and decrypt the passport data encrypted with the private key; see column 8, lines 40-42; MY-USER-ID).

As per claim 54, Fortenberry et al. moreover point out:

selecting at least one set of information objects, comprising at least one piece of the first party's information (see column 8, lines 1-7; access to information may be granted at various levels such as real-ID (very secure), virtual-ID and less private information classes); and

creating a key to authorized access of the selected set of information objects (see column 8, lines 1-7; several securities keys for access to information at various levels).

As per claim 55, Fortenberry et al. then describe:

selecting the characteristics of the second party that can present the authorization key for information (see column 8, lines 29-31; figure 5, process block 502; user requests transaction with particular web site; see column 7, lines 2-6; virtual information may include user's preferences, tastes, goals for visiting web sites, etc.).

As per claim 56, Fortenberry et al. moreover suggest:

Encoding the authorization key with at least one of a plurality of attributes (see column 8, lines 37-42; figure 5, process block 508; request for information includes MY-USER-ID and INTERNET-SITE).

As per claim 57, Fortenberry et al. additionally specify that the at least one of the plurality of attributes includes an attribute of the second party presenting the authorization key to access the first party's information (see column 8, lines 37-42; figure 5, process block 508; request for information includes MY-USER-ID and INTERNET-SITE).

As per claim 58, Fortenberry et al. next mention:

altering the first party's personal information (see column 7, lines 10-14; at the user's option, virtual information can be converted to real information becoming restricted and not longer publicly available); and

storing the altered personal information in the database (see column 6, lines 52-57; figure 3, item 305; first data field contains real information).

As per claim 59, Fortenberry et al. also describe:

designating an entity to receive altered personal information (see column 8, lines 29-32; figure 5, process blocks 502 and 504; user requests transaction with a particular vendor and provides public key); and

transmitting the altered personal information to the designated entity (see column 8, lines 57-59, figure 5, process block 516; requested information is sent to the vendor).

As per claim 60, Fortenberry et al. further discuss:

Transmitting the information object via a communication network to a device coupled to the communication network (see column 6, lines 30-32; figure 2, items 210, 216, and 208; web

sit receives the encrypted user information from the passport agent; column 5, lines 51-52; figure 2A, items 210a-210n; coupled to the Internet is a plurality of web sites).

As per claim 62, Fortenberry et al. then specify:

transmitting the information object via public key encryption (see column 8, lines 54-59; figure 5, process block 516; the private key is used to encrypt the passport which is sent to the vendor).

As per claim 63, Fortenberry et al. further embody:

first party's personal information including first party's contact information (see column 6, lines 52-55; user's real name, address), internet preferences (see column 7, lines 4-5; goals for visiting web sites and preferences), or preferences for billing or payment methods (see column 6, line54-55; credit card information).

As per claim 64, Fortenberry et al. next describe:

receiving an authorization key for the second party (see column 8, lines 37-42; figure 5, process block 508; vendor submits request for information which includes MY-USER-ID).

As per claim 65, Fortenberry et al. also point out:

authenticating the second party (see column 8, lines 46-51; figure 5, process block 512; passport agent determines whether or not the requested information should be transmitted to the vendor in encrypted form).

As per claim 68, Fortenberry et al. depict a method for securing a first party's personal information comprising:

entering the first party's personal information comprising at least one of a plurality of information objects (see column 6, lines 52-55; figure 3, item 305; real information about a user such as the user's real name, address, credit card information, social security number, etc.; column 6, lines 63-67; column 7, lines 1-9; figure 3, item 305; virtual information includes user's preferences); and

assigning, by the first party, at least one of a plurality of security levels to each information object at any granularity to each one of the at least one of a plurality of information objects (see column 7, lines 24-30; figure 3, items 304 and 306; security level is assigned to each item of the user information included in the passport data field; see column 7, lines 53-60; security levels assigned to each item of user information range from highly secure to public, for a high security level of 100 on an exemplary scale of 0-100 levels to public level 0).

As per claim 69, Fortenberry et al. illustrate a program storage device readable by a processor embodying a program of instructions executable by the processor to perform secure delivery of a first party's personal information comprising:

storing the first party's personal information comprising at least one of a plurality of information objects (see column 6, lines 52-55; figure 3, item 305; real information about a user such as the user's real name, address, credit card information, social security number, etc.;

column 6, lines 63-67; column 7, lines 1-9; figure 3, item 305; virtual information includes user's preferences);

associating, by the first party, each one of the plurality of information objects with at least one of a plurality of security clearance levels at any granularity(see column 7, lines 24-30; figure 3, items 304 and 306; security level is assigned to each item of the user information included in the passport data field; see column 7, lines 53-60; security levels assigned to each item of user information range from highly secure to public, for a high security level of 100 on an exemplary scale of 0-100 levels to public level 0);

receiving a request message to access the first party's personal information, comprising an authorization key to access a first portion of the first party's personal information (see column 8, lines 37-46; figure 5, process block 508; vendor requests relevant information in a message that looks like: RELEASE SOCIAL-SECURITY-NUMBER TO WEB-SITE-X ON BEHALF OF MY-USER-ID, where SOCIAL-SECURITY-NUMBER in combination with MY-USER-ID forms an authorization key),

comprising an authorization key to access a first portion of the first party's personal information (see column 8, lines 46-55; figure 5, process blocks 510, 512, and 514; vendor receives request and determines encryption key for requested data; see column 7, lines 52-58; figure 4, process block 410; column 8, lines 1-7; and figure 3, item 308; the security levels assigned to the user's data have a corresponding security key (i.e. a first portion of first party's personal information that the authorization code accesses) stored in the key field of the passport),

where the authorization key is indicative of a second security clearance level (see column 8, lines 37-46; figure 5, process block 508; see column 7, lines 52-58; figure 4, process block 410; where the social security number for my user id has a user assigned security level);

comparing the first security clearance level and the second security clearance level to determine an appropriate overall clearance level (column 8, lines 46-57; figure 5, process block 512; column 8, lines 1-7; passport agent finds the security level of the requested data, the second security clearance level, in order to find the security used for encrypting that particular data at the user assigned security level, the first security clearance level);

matching the request message and the overall clearance level with a second portion of the first party's personal information (see column 8, lines 46-57; figure 5, process blocks 512 and 514; based on the security level of the identified information (i.e. the overall security clearance level), determining the encryption for the information appropriate to that level; column 8, lines 1-7 and 54-58; figure 5, process block 514; where the encrypted data results for a security key for that level and represents a second portion of the first party's personal information); and

securely transmitting the second portion of the first party's personal information (see column 8, lines 55-64; figure 5, process block 516; the vendor receives the encrypted passport data requested).

As per claim 70, Fortenberry et al. further elaborate on:

authenticating the request message (see column 8, lines 46-51; figure 5, process block 512; passport agent determines whether or not the requested information should be transmitted to the vendor in encrypted form).

As per claim 74, Fortenberry et al. then point out:

generating an authorization key (see column 7, lines 24-33; figure 3, item 308; figure 4, process 416; storing generated keys for encryption and decryption in a key field and assigning an encryption key);

providing the authorization key to the second party (see column 8, lines 1-7; security keys for each item at different security levels are delivered to the passport requestor); and

encoding the authorization key with at least one of a plurality of criteria (see column 8, lines 1-7; security keys for each item at different security levels are delivered to the passport requestor; see column 9, lines 8-10; the public and private keys described herein may be encrypted using the double keying encryption technology currently known in the art).

As per claim 75, Fortenberry et al. moreover show:

where the at least one of a plurality of criteria includes a criterion to indicate the information that can be accessed by the second party with the authorization key (see column 8, lines 1-7; security key at a level corresponding to security level of any or real-ID, virtual-ID and less private information).

As per claim 77, Fortenberry et al. further suggest:

where the at least one of a plurality of criteria includes a criterion designating the category of the first party's personal information that can be accessed by the second party using the authorization key (see column 8, lines 1-7; security key at a level corresponding to security

level of any or real-ID, virtual-ID and less private information including the category of information that can be decrypted by that key).

Claim Rejections - 35 USC § 103

11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

12. Claim 52 is rejected under 35 U.S.C. 103(a) as being unpatentable over Fortenberry, U.S. Patent No. 6,005,939 A as applied to claim 48 above, and further in view of Ho, U.S. Patent No. 6,148,342 A.

Fortenberry et al. disclose the method for disbursing a first party's personal information of claim 48. However, they do not explicitly teach recording every access of the first party's personal information. Ho discusses recording every access of the first party's personal information to create an audit trail (see column 5, lines 27-30 and figure 1, items 156 and 104; identifier database maintains log which may store that a query was received from a certain user; see column 5, lines 36-38; figure 1, item 156; third party auditor can check the first log for irregularities). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the method of Fortenberry et al. with the recording every access of Ho to determine the integrity of the system by checking for irregularities (see column 5, lines 36-38).

13. Claim 61 is rejected under 35 U.S.C. 103(a) as being unpatentable over Fortenberry, U.S. Patent No. 6,005,939 A as applied to claim 60 above, and further in view of Moozakis, "Internet Printing Takes Hold."

Fortenberry et al. disclose the method for disbursing a first party's personal information of claim 60. However, they do not show Internet Printing Protocol. Moozakis describes a printer coupled to the communication network directly via the Internet Printing Protocol (see entire article; IPP as a mechanism for transmission of information directly to a printer for distribution of information). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the method of Fortenberry et al. with the IPP of Moozakis as an efficient manner for distributing information (see entire article).

14. Claim 62 is rejected under 35 U.S.C. 103(a) as being unpatentable over Fortenberry, U.S. Patent No. 6,005,939 A as applied to claim 48 above, and further in view of Rozen et al., U.S. Patent No. 6,073,342 A.

Fortenberry et al. disclose the method for disbursing a first party's personal information of claim 48. Although they point out transmitting the information object via public key encryption (see column 8, lines 54-59; figure 5, process block 516; the private key is used to encrypt the passport which is sent to the vendor), they do not teach using secure E-mail. Rozen et al. describes transmitting the object information via secure E-mail (see column 8, lines 59-65 ; information via mail; column 7, lines 37-39; that is secure). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to

combine the method of Fortenberry et al. with the secure E-mail of Rozen et al. to insure integrity and privacy of the information exchange (see column 7, lines 35-39).

15. Claims 66 and 67 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fortenberry, U.S. Patent No. 6,005,939 A as applied to claim 48 above, and further in view of Ho, U.S. Patent No. 6,148,342 A.

As per claim 66, Fortenberry et al. disclose the method for disbursing a first party's personal information of claim 48. However, they do not explicitly teach a query in executable form. Ho discusses receiving a query for the first party's information in a readily executable form (see column 3, lines 40-43 and line 67; column 4, lines 1-2; figure 1, items 104, 116, 112, and 132; identifier in request for data serves as a search key to query the database). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the method of Fortenberry et al. with the executable query of Ho to query the database for the requested information (see column 4, lines 1-2).

As per claim 67, Ho further points out periodically generating a report on the transmittal of information (see column 5, lines 30-35; figure 1, items 152, 164, and 104; a second log wich records the subject internal I.D. operate upon, the destination to which the requested information was sent, and the source terminal I.D.). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the method of

Fortenberry et al. with the report on transmittal of information of Ho to determine the integrity of the system by checking for irregularities (see column 5, lines 36-38).

16. Claim 71 is rejected under 35 U.S.C. 103(a) as being unpatentable over Fortenberry, U.S. Patent No. 6,005,939 A as applied to claim 69 above, and further in view of Ho, U.S. Patent No. 6,148,342 A.

Fortenberry et al. disclose the program storage device of claim 69. However, they do not explicitly teach an audit trail every access of the first party's personal information. Ho discusses recording every access of the first party's personal information to create an audit trail (see column 5, lines 27-30 and figure 1, items 156 and 104; identifier database maintains log which may store that a query was received from a certain user; see column 5, lines 36-38; figure 1, item 156; third party auditor can check the first log for irregularities). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the program storage device of Fortenberry et al. with the recording every access of Ho to determine the integrity of the system by checking for irregularities (see column 5, lines 36-38).

17. Claims 72 and 73 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fortenberry, U.S. Patent No. 6,005,939 A as applied to claim 70 above, and further in view of Ho, U.S. Patent No. 6,148,342 A.

As per claim 72, Fortenberry et al. disclose the program storage device of claim 70. However, they do not explicitly teach an audit trail every access of the first party's personal

information. Ho discusses recording every access of the first party's personal information to create an audit trail (see column 5, lines 27-30 and figure 1, items 156 and 104; identifier database maintains log which may store that a query was received from a certain user; see column 5, lines 36-38; figure 1, item 156; third party auditor can check the first log for irregularities). Ho additionally points out recording an identifier to identify a party that receives the first party's personal information (see column 5, lines 30-35; figure 1, items 152 and 164; log includes the destination to which the requested information was send and the source terminal I.D. for auditing). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the program storage device of Fortenberry et al. with the recording every access of Ho to determine the integrity of the system by checking for irregularities (see column 5, lines 36-38).

As per claim 73, Ho then discusses recording an identifier to identify a second party (see column 5, lines 30-35; figure 1, items 152 and 164; log includes the destination to which the requested information was send and the source terminal I.D. for auditing). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the program storage device of Fortenberry et al. with the recording every access of Ho to determine the integrity of the system by checking for irregularities (see column 5, lines 36-38).

Allowable Subject Matter

18. Claims 50, 51, and 76 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

19. The following is a statement of reasons for the indication of allowable subject matter:

Claims 50 and 51 are drawn to a method for disbursing a first party's personal information to a second party. The closest prior art, Fortenberry et al., U.S. Patent No. 6,005,939 A, discloses a similar method. Although Fortenberry et al. describe obtaining a second party identifier (see column 8, lines 42-47; figure 5, process block 510; vendor requests: RELEASE-TYPE TO INTERNET-SITE ON BEHALF OF MY-USER-ID), they neither teach nor suggest recording the second party identifier if the second party is not authorized to receive the information, nor rejecting the second party's request for information. These limitations explicitly incorporated in intervening claim 50 renders claims 50 and 51 to have allowable subject matter.

Claim 76 is drawn to a method for disbursing a first party's personal information to a second party. The closest prior art, Fortenberry et al., U.S. Patent No. 6,005,939 A, discloses a similar method. Although Fortenberry et al. describe encoding the authorization key with at least one of a plurality of criteria (see column 8, lines 1-7; security keys for each item at different security levels are delivered to the passport requestor; see column 6, lines 30-36; figure 2B, item 210; web site receives keys from user in transmission packet; see column 9, lines 8-10; where the public keys are encrypted using double keying encryption technology), they neither show nor motivate the at least one of a plurality of criteria includes a criterion to indicate the number of

times the authorization key can be use by the second party to obtain access. This limitation explicitly incorporated into dependent claim 76 renders it to have allowable subject matter.

Conclusion

20. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Telephone Inquiry Contacts

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Justin T. Darrow whose telephone number is (703) 305-3872 and whose electronic mail address is justin.darrow@uspto.gov. The examiner can normally be reached Monday-Friday from 8:30 AM to 5:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barrón, Jr., can be reached at (703) 305-1830.

The fax number for Formal or Official faxes to Technology Center 2100 is (703) 872-9306. In order for a formal paper transmitted by fax to be entered into the application file, the paper and/or fax cover sheet must be signed by a representative for the applicant. Faxed formal papers for application file entry, such as amendments adding claims, extensions of time, and statutory disclaimers for which fees must be charged before entry, must be transmitted with an authorization to charge a deposit account to cover such fees. It is also recommended that the cover sheet for the fax of a formal paper have printed "**OFFICIAL FAX**". Formal papers transmitted by fax usually require three business days for entry into the application file and consideration by the examiner. Formal or Official faxes including amendments after final rejection (37 CFR 1.116) should be submitted to (703) 872-9306 for expedited entry into the application file. It is further recommended that the cover sheet for the fax containing an amendment after final rejection have printed not only "**OFFICIAL FAX**" but also "**AMENDMENT AFTER FINAL**".

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Any inquiry of a general nature or relating to the status of this application should be directed to the Group receptionist whose telephone number is (703) 305-3900.

February 9, 2004

Justin Darrow

JUSTIN T. DARROW
PRIMARY EXAMINER
TECHNOLOGY CENTER 2100